embodiments differ from the embodiments disclosed herein in Sections II and III as follows. The identifier holder, e.g., the telephone number owner or email address user, takes the place of registrant **202**. The entity that provides the identifier, e.g., a phone company for a telephone number or an email provider for an email identifier, takes the place of registry **102**. A facilitating company may take the place of registrar **104**. The facilitating company may have or may establish a communication channel with the entity that provides the identifier, e.g., the entity that provides the identifier has an internet-based interface or API.

For the setup phase of such embodiments, method **100** proceeds as disclosed above in Section II, except that the entity that provides the identifier performs the actions of registry **102**, and the facilitating company performs the actions of registrar **104**. Instead of registry **102** adding support for a registrar of record proof EPP extension, the entity that provides the identifier provides support for responding to requests **208** for proof sent by the facilitating company. The requests may be sent through the communication channel between the entity that provides the identifier and the facilitating company. In such embodiments, the entity that provides the identifier obtains and utilizes a proof key pair as disclosed above in Section III. The registry signature verification program **106** may be configured to verify the signatures by the entity that provides the identifier, rather than signatures by registry **102**. The signatures may be on data that specifies an identifier such as a phone number or email address and an existing blockchain address, instead of on data that specifies a domain name and an existing blockchain user address.

For the execution phase of such embodiments, the entity that provides the identifier performs the actions of registry **102**, and the facilitating company performs the actions of registrar **104**. Any of methods **200**, **300**, **400**, or **500** may be altered as described presently. The identifier holder, instead of registrant **202**, requests **206** assignment of their identifier as a blockchain user address. The facilitating company receives the request and requests **208** proof from the entity that provides the identifier. The remaining flow is as described above in Section II for any of methods **200**, **300**, **400**, or **500**, mutatis mutandis.

According to some embodiments, the facilitating company may be merged with the entity that provides the identifier. In such embodiments, the entity that provides the identifier may establish an interface that performs the analogous actions of registrar **104**. Further, the request **208** for proof may be performed essentially in-house. Such embodiments perform as described herein, except that communications **208**, **210**, and **212** are performed by different portions of the same entity, rather than by different entities.

Embodiments disclosed in this subsection may have the added benefit of enabling secure two-factor identification by consulting the blockchain for a given blockchain network participant's address to fetch additional factors for use to verify their identity. For example, if a given address on a blockchain has an attached phone number or email address, those could be consulted on chain as a source to send a message to, to confirm proof of address ownership.

Further, embodiments disclosed in this subsection may be particularly beneficial to payment providers and their users. As used herein, the term "payment provider" refers to any entity that provides customer accounts to customers that permit such customers to send to and receive payment from other customers using customer identifiers instead of banking information. For example, a payment provider may enable its customers to send and receive money amongst themselves by specifying domain names and currently amounts. In particular, a first customer may log into a payment provider webpage interface by providing a domain name and password, then provide to the interface a domain name of a second customer, as well as a US dollar amount, along with instructions to pay, and the payment provider may respond to such instruction by moving currency between customer accounts as instructed. According to embodiments described in this subsection, a payment provider may assign an existing payment provider identifier (e.g., domain name) as blockchain address. In this way, a payment provider customer may broadcast, publish, or otherwise make known a central payment identifier, e.g., their domain name, along with instructions that the customer may receive payment through such identifier either by way of the standard techniques of the payment provider, or via cryptocurrency using a cryptocurrency blockchain network using the same identifier, e.g., domain name.

Certain embodiments can be performed using a computer program or set of programs. The computer programs can exist in a variety of forms both active and inactive. For example, the computer programs can exist as software program(s) comprised of program instructions in source code, object code, executable code or other formats; firmware program(s), or hardware description language (HDL) files. Any of the above can be embodied on a transitory or non-transitory computer readable medium, which include storage devices and signals, in compressed or uncompressed form. Exemplary computer readable storage devices include conventional computer system RAM (random access memory), ROM (read-only memory), EPROM (erasable, programmable ROM), EEPROM (electrically erasable, programmable ROM), and magnetic or optical disks or tapes.

While the invention has been described with reference to the exemplary embodiments thereof, those skilled in the art will be able to make various modifications to the described embodiments without departing from the true spirit and scope. The terms and descriptions used herein are set forth by way of illustration only and are not meant as limitations. In particular, although the method has been described by examples, the steps of the method can be performed in a different order than illustrated or simultaneously. Those skilled in the art will recognize that these and other variations are possible within the spirit and scope as defined in the following claims and their equivalents.

What is claimed is:

1. A domain name system (DNS) registry facilitated method of assigning a domain name registered to a registrant as a blockchain address in a blockchain network, the method comprising:

obtaining, by the DNS registry for the domain name, a cryptographic asymmetric proof key pair comprising a public key and a private key;

providing, by the DNS registry, the public key and a computer executable registry signature verification program for addition to a block in a blockchain of the blockchain network, wherein the registry signature verification program is configured to use the public key to validate signatures made using the private key;

receiving, by the DNS registry, a request for a proof of registrar of record for the domain name from a registrar, wherein the request comprises the domain name;

confirming, by the DNS registry, that the registrar is a registrar of record for the domain name;

providing, by the DNS registry, a proof of registration message, wherein the proof of registration message